PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-321748
(43)Date of publication of application : 12.12.1997

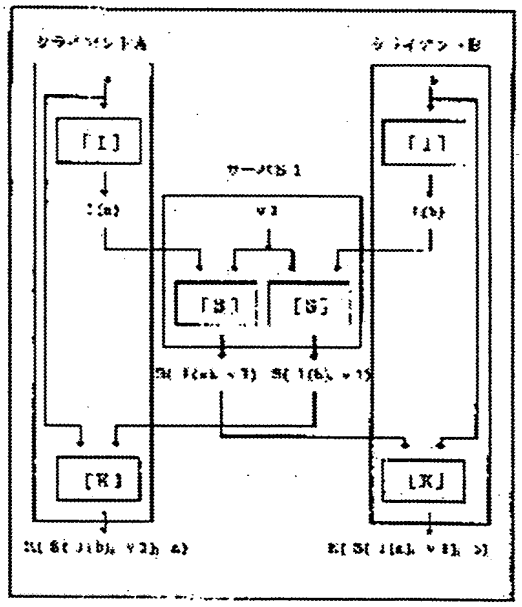
(51)Int.CI. H04L 9/08
G09C 1/00
G09C 1/00

(21)Application number : 08-154991
(22)Date of filing : 27.05.1996

(71)Applicant : TRANS KOSUMOSU KK
(72)Inventor : OKUDA MASATAKA
ISHIOKA HIDEAKI

(54) COMMUNICATION SYSTEM BY SHARED CRYPTOGRAPHIC KEY, SERVER DEVICE AND CLIENT DEVICE FOR THE SYSTEM, AND METHOD FOR SHARING CRYPTOGRAPHIC KEY IN COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To enable the operation of a system for changing a cryphotograpic key to be shared at a short time interval and to rapidly improve the stability of the cryptographic system by changing the shared cryptographic key only by means of the change of a control variable in a server while a password at a client side is foxed.
SOLUTION: A client A generates specific is I(a) through the use of a specific is generating algorithm (I) and informs it to the server S1. The server S1 generates the open idS(I(b), v1) of the client B through the use of an open is generating algorithm (S) with the control variable v1 which is secretly managed by the server S1 as an input and reports it to the client A. The client A generates the cryptographic key K(S(I(b), v1), a) through the use of a cryptographic key generating algorithm (K) with the open is S(I(b), v1) of the client B and the self secret password (a) as the input.



LEGAL STATUS

[Date of request for examination] 04.06.1998
[Date of sending the examiner's decision of rejection] 27.12.2001
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－321748

(43)公開日　平成９年(1997)12月12日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｄ	
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｄ	
			7259－5Ｊ			６３０Ｅ	
		６６０	7259－5Ｊ			６６０Ｅ	
				Ｈ０４Ｌ	9/00	６０１Ｅ	

審査請求　未請求　請求項の数９　ＦＤ　（全 13 頁）

(21)出願番号　特願平8－154991

(22)出願日　平成８年(1996)５月27日

(71)出願人　396011831
トランス・コスモス株式会社
東京都港区赤坂３丁目３番３号

(72)発明者　奥田　昌孝
東京都渋谷区猿楽町17－16　代官山フォーラム301

(72)発明者　石岡　英明
千葉県市川市柏井町１－1229－41

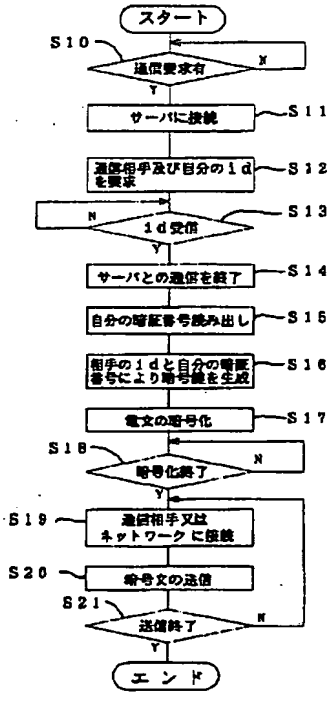
(74)代理人　弁理士　二瓶　正敬

(54)【発明の名称】　共有暗号鍵による通信システム、同システム用サーバ装置、同システム用クライアント装置、及び通信システムにおける暗号鍵の共有方法

(57)【要約】

【課題】　不特定多数との暗号通信に適していて、全エンティティが共通の鍵を共有することが可能で、また、安全のため公開情報を変える場合、自分の秘密情報を変更する必要がない共有暗号鍵による通信システムを提供する。

【解決手段】　クライアント（Ａ，Ｂ）側の暗証番号は一定のまま、サーバ（Ｓ１）の制御変数ｖ１の変更のみで共有する暗号鍵Ｋを変更できるようにしている。このため、短い時間間隔で、共有する暗号鍵を変化させるシステム運用が可能となり、暗号システムの安全性が飛躍的に向上する。また、サーバの制御変数をある特定の値に設定することでサーバ所属のクライアントグループ内で同じ暗号鍵を共有できるようにしている。このため、緊急時など、特別な状況においてサーバの制御のみでグループ内の暗号化を解除することができる



【特許請求の範囲】

【請求項１】　少なくともクライアントＡ、クライアントＢ、サーバＳ１により構成される共有暗号鍵による通信システムであって、

前記クライアントＡは、予め定めた自分の暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］、並びに暗号鍵生成アルゴリズム［Ｋ］を保持する記憶手段と、前記暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ａ）を生成する手段と、生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知する手段と、前記クライアントＢとの共通鍵を生成するために、前記サーバＳ１へ前記クライアントＢの公開ｉｄを要求する手段と、前記サーバＳ１から送信される前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）と前記暗証番号ａを入力として前記暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｉ（ｂ），ｖ１），ａ）を生成する手段とを有し、

前記クライアントＢは、予め定めた自分の暗証番号ｂ及び固有ｉｄ生成アルゴリズム［Ｉ］、並びに暗号鍵生成アルゴリズム［Ｋ］を保持する記憶手段と、前記暗証番号ｂ及び固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ｂ）を生成する手段と、生成された固有ｉｄ　Ｉ（ｂ）を前記サーバＳ１へ通知する手段と、前記サーバＳ１又は前記クライアントＡ及びクライアントＢが接続されたネットワーク経由で前記クライアントＡの公開ｉｄを入手し、前記クライアントＡの公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）と前記暗証番号ｂを入力として前記暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｉ（ａ），ｖ１），ｂ）を生成する手段とを有し、

前記サーバＳ１は制御変数ｖ１を生成する手段と、前記クライアントＡから通知された固有ｉｄ　Ｉ（ａ）及び前記クライアントＢから通知された固有ｉｄＩ（ｂ）を保持するとともに、秘密で管理する前記制御変数ｖ１並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記クライアントＡからの要求を受けたときは、前記クライアントＢの固有ｉｄ　Ｉ（ｂ）と前記制御変数ｖ１と、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）を生成する手段と、生成された前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）を前記クライアントＡに送信する手段と、前記クライアントＡの固有ｉｄ　Ｉ（ａ）と前記制御変数ｖ１、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＡの前記公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）を生成する手段と、生成された前記公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）を前記クライアントＡに送信する手段とを有し、

前記アルゴリズム［Ｉ］、［Ｓ］、［Ｋ］がＫ（Ｓ（Ｉ（ｂ），ｖ１），ａ）＝Ｋ（Ｓ（Ｉ（ａ），ｖ１），ｂ）を満足するものである共有暗号鍵による通信システム。

【請求項２】　前記サーバ装置が制御変数ｖ１を生成する手段と、前記クライアントＡから通知された固有ｉｄ　Ｉ（ａ）及び前記クライアントＢから通知された固有ｉｄ　Ｉ（ｂ）を保持するとともに、秘密で管理する前記制御変数ｖ１並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記クライアントＡからの要求を受けたときは、前記クライアントＢの固有ｉｄ　Ｉ（ｂ）と前記制御変数ｖ１と、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）を生成する手段と、生成された前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）を前記クライアントＡに送信する手段と、前記クライアントＡの固有ｉｄ　Ｉ（ａ）と前記制御変数ｖ１、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＡの前記公開ｉｄＳ（Ｉ（ａ），ｖ１）を生成する手段と、生成された前記公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）を前記クライアントＡに送信する手段とを有するものである請求項１記載の共有暗号鍵による通信システム用サーバ装置。

【請求項３】　前記クライアント装置が予め定めた自分の暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］、並びに暗号鍵生成アルゴリズム［Ｋ］を保持する記憶手段と、前記暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ａ）を生成する手段と、生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知する手段と、前記クライアントＢとの共通鍵を生成するために、前記サーバＳ１へ前記クライアントＢの公開ｉｄを要求する手段と、前記サーバＳ１から送信される前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）と前記暗証番号ａを入力として前記暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｉ（ｂ），ｖ１），ａ）を生成する手段とを有する請求項１記載の通信システム用クライアント装置。

【請求項４】　少なくともクライアントＡ、クライアントＢ、サーバＳ１により構成される通信システムにおける暗号鍵の共有方法であって、

前記クライアントＡが、前もって自分の暗証番号ａを定め、固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ａ）を生成するステップと、

生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知するステップと、

前記クライアントＢが、前もって自分の暗証番号ｂを定め、固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ｂ）を生成するステップと、

生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知するステップと、

前記クライアントＡが、前記クライアントＢとの共通鍵を生成するために、前記サーバＳ１へ前記クライアントＢの公開ｉｄを要求するステップと、

前記サーバＳ１が前記クライアントＡからの要求を受

け、保有している前記クライアントＢの固有ｉｄ　Ｉ（ｂ）と前記サーバが秘密で管理している制御変数ｖ１を入力として、公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）を生成するステップと、
生成された前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）を前記クライアントＡに送信するステップと、
前記サーバＳ１が、保有している前記クライアントＡの固有ｉｄ　Ｉ（ａ）とｖ１から前記クライアントＡの公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）を生成するステップと、
生成された前記クライアントＡの公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）を前記クライアントＡに送信するステップと、
前記クライアントＡが入手した前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）と前記暗証番号ａを入力として暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｉ（ｂ），ｖ１），ａ）を生成するステップと、
前記クライアントＢが前記サーバＳ１又は前記クライアントＡ及び前記クライアントＢの接続されたネットワーク経由で前記クライアントＡの公開ｉｄを入手し、暗号鍵　Ｋ（Ｓ（Ｉ（ａ），ｖ１），ｂ）を生成するステップとを、
有し、
前記アルゴリズム［Ｉ］、［Ｓ］、［Ｋ］がＫ（Ｓ（Ｉ（ｂ），ｖ１），ａ）＝Ｋ（Ｓ（Ｉ（ａ），ｖ１），ｂ）を満足するものである通信システムにおける暗号鍵の共有方法。

【請求項５】　少なくともサーバＳ１に管理されるクライアントＡ、サーバＳ２に管理されるクライアントＣ、前記サーバＳ１と前記サーバＳ２を管理する親サーバＳ３により構成される共有暗号鍵による通信システムであって、
前記クライアントＡは、予め定めた自分の暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］、並びに暗号鍵生成アルゴリズム［Ｋ］を保持する記憶手段と、前記暗証番号ａ及び前記固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ａ）を生成する手段と、生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知する手段と、前記クライアントＣとの共通鍵を生成するために、前記サーバＳ１へ前記クライアントＣの公開ｉｄを要求する手段と、前記サーバＳ１から送信される前記クライアントＣの３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）と前記暗証番号ａを入力として前記暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１），ａ）を生成する手段とを有し、
前記クライアントＣは、予め定めた自分の暗証番号ｃ及び固有ｉｄ生成アルゴリズム［Ｉ］、並びに暗号鍵生成アルゴリズム［Ｋ］を保持する記憶手段と、前記暗証番号ｃ及び固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ｃ）を生成する手段と、生成された固有ｉｄ　Ｉ（ｃ）を前記サーバＳ２へ通知する手段と、前記クライアントＡ及びクライアントＣが接続されたネットワーク経由で前記クライアントＡの３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ａ），ｖ１），ｖ３），ｖ２）を入手し、前記クライアントＡの前記３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ａ），ｖ１），ｖ３），ｖ２）と前記暗証番号ｃを入力として前記暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ａ），ｖ１），ｖ３），ｖ２），ｃ）を生成する手段とを有し、
前記サーバＳ１は前記クライアントＡから通知された固有ｉｄ　Ｉ（ａ）を保持するとともに、秘密で管理する制御変数ｖ１並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記クライアントＡからの要求を受けたときは、要求相手が自グループに属するか否かを判断する手段と、自グループに属さない要求相手のときは前記親サーバＳ３に前記クライアントＡからの要求を転送する手段と、前記親サーバＳ３から受信した前記クライアントＣの２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）と、前記制御変数ｖ１と、前記公開ｉｄ生成アルゴリズム［Ｓ］から前記３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）を生成して前記クライアントＡに送信する手段とを有し、
前記サーバＳ２は前記クライアントＣから通知された固有ｉｄ　Ｉ（ｃ）を保持するとともに、秘密で管理する制御変数ｖ２並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記親サーバＳ３からの要求を受けたときは、前記クライアントＣの固有ｉｄ　Ｉ（ｃ）と前記制御変数ｖ２と、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＣの１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ２）を生成する手段と、生成された前記クライアントＣの１次公開ｉｄＳ（Ｉ（ｃ），ｖ２）を前記親サーバＳ３に送信する手段とを有し、
前記親サーバＳ３は前記サーバＳ２から送信された前記クライアントＣの１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ２）を保持するとともに、秘密で管理する制御変数ｖ３並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記サーバＳ１からの要求を前記サーバＳ２に転送する手段と、前記サーバＳ２から前記クライアントＣの１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ２）を受けたときは、前記制御変数ｖ３と、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＣの前記２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）を生成する手段と、生成された前記クライアントＣの２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）を前記サーバＳ１に送信する手段とを有し、
前記アルゴリズム［Ｉ］、［Ｓ］、［Ｋ］がＫ（Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１），ａ）＝Ｋ

（Ｓ（Ｓ（Ｓ（Ｉ（ａ），ｖ１），ｖ３），ｖ２），ｃ）を満足するものである共有暗号鍵による通信システム。

【請求項６】　前記サーバＳ１が、前記クライアントＡから通知された固有ｉｄ　Ｉ（ａ）を保持するとともに、秘密で管理する制御変数ｖ１並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記クライアントＡからの要求を受けたときは、要求相手が自グループに属するか否かを判断する手段と、自グループに属さない要求相手のときは前記親サーバＳ３に前記クライアントＡからの要求を転送する手段と、前記親サーバＳ３から受信した前記クライアントＣの２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）と、前記制御変数ｖ１と、前記公開ｉｄ生成アルゴリズム［Ｓ］から前記３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）を生成して前記クライアントＡに送信する手段とを有する請求項５記載の通信システム用サーバ装置。

【請求項７】　前記親サーバＳ３が、前記サーバＳ２から送信された前記クライアントＣの１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ２）を保持するとともに、秘密で管理する制御変数ｖ３並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記サーバＳ１からの要求を前記サーバＳ２に転送する手段と、前記サーバＳ２から前記クライアントＣの１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ２）を受けたときは、前記制御変数ｖ３と、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＣの前記２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）を生成する手段と、生成された前記クライアントＣの２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）を前記サーバＳ１に送信する手段とを有する請求項５記載の通信システム用サーバ装置。

【請求項８】　前記クライアント装置が、予め定めた自分の暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］、並びに暗号鍵生成アルゴリズム［Ｋ］を保持する記憶手段と、前記暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ａ）を生成する手段と、生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知する手段と、前記クライアントＣとの共通鍵を生成するために、前記サーバＳ１へ前記クライアントＣの公開ｉｄを要求する手段と、前記サーバＳ１から送信される前記クライアントＣの３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）と前記暗証番号ａを入力として前記暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１），ａ）を生成する手段とを有する請求項５記載の通信システム用クライアント装置。

【請求項９】　少なくともサーバＳ１に管理されるクライアントＡ、サーバＳ２に管理されるクライアントＣ、前記サーバＳ１と前記サーバＳ２を管理する親サーバＳ３により構成される通信システムにおける暗号鍵の共有方法であって、

前記クライアントＡが、前もって自分の暗証番号ａを定め、固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ａ）を生成するステップと、

生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知するステップと、

前記クライアントＣが、前もって自分の暗証番号ｃを定め、固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ｃ）を生成するステップと、

生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ２へ通知するステップと、

前記クライアントＡが、前記クライアントＣとの共通鍵を生成するために、前記サーバＳ１へ前記クライアントＣの公開ｉｄを要求するステップと、

要求された通信相手である前記クライアントＣが自グループに属するか否かを前記サーバＳ１が判断するステップと、

前記クライアントＣが自グループに属さないときは、前記サーバＳ１が前記親サーバＳ３へ前記クライアントＣの公開ｉｄを要求するステップと、

前記親サーバＳ３が、前記サーバＳ１から要求された前記クライアントＣを管理するサーバＳ２へＣの公開ｉｄを要求するステップと、

前記サーバＳ２が、保有している前記クライアントＣの固有ｉｄ　Ｉ（ｃ）と自らの制御変数ｖ２を入力としてアルゴリズム［Ｓ］を用いて、前記クライアントＣの１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ　２）を生成するステップと、

前記サーバＳ２が、生成された前記１次公開ｉｄを前記親サーバＳ３へ送信するステップと、

前記親サーバＳ３が、前記１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ２）と自らの制御変数ｖ３を入力としてアルゴリズム［Ｓ］を用いて、２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）を生成するステップと、

前記親サーバＳ３が生成された前記２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）を前記サーバＳ１へ送信するステップと、

前記サーバＳ１が前記２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）と前記制御変数ｖ１と前記アルゴリズム［Ｓ］を用いて、３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）を生成するステップと、

前記サーバＳ１が、生成された前記３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）を前記クライアントＡへ送信するステップと、

前記クライアントＡが前記３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）と前記暗証番号ａとアルゴリズム［Ｋ］を用いて暗号鍵Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１），ａ）を生成するステップと、

前記クライアントＣが前記暗証番号ｃとアルゴリズム［Ｋ］を用いて暗号鍵Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ａ），ｖ１），ｖ３），ｖ２），ｃ）を生成するステップとを有し、

前記アルゴリズム［Ｉ］、［Ｓ］、［Ｋ］がＫ（Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１），ａ）＝Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ａ），ｖ１），ｖ３），ｖ２），ｃ）を満足するものである通信システムにおける暗号鍵の共有方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信システムにおける暗号通信に関し、特に有線、無線のコンピュータネットワーク、移動体通信システムなどにおける通信文の暗号化とその復号における暗号鍵の共有方法の改良に関する。

【０００２】

【従来の技術】

【表１】従来から各種の暗号鍵の共有方法があるが、これらの概略は次のとおりである（図７～９参照）。

＜第１の方法＞各エンティティが想定される全ての通信相手と個別に暗号鍵を共有する方法。

＜第２の方法＞各エンティティが自分の秘密情報に基づき公開情報を作成し、これを読み出し自由であるが書き込みや消去は厳密に管理された公開ファイルに登録し、通信の際に自分の秘密情報と相手の公開情報から共有すべき暗号鍵を計算により求める方法。

＜第３の方法＞各エンティティの公開識別子を基にセンターが各エンティティの秘密アルゴリズムを作成し配送する準備をした後、通信相手の公開識別子と自分の秘密アルゴリズムから共有すべき暗号鍵を計算して求める方法。

【０００３】

【発明が解決しようとする課題】

【表２】

＜第１の方法の問題＞第１の方法では、想定される通信相手の数が多いと管理に多大な手間を要し、不特定多数との暗号通信には不向きである。

＜第２の方法の問題＞第２の方法では、全エンティティが共通の鍵を共有することはできない。また、安全のため公開情報を変える場合、自分の秘密情報も変える必要があり管理しにくい。

＜第３の方法の問題＞第３の方法では、事前準備として各エンティティへ秘密アルゴリズムを配送する必要があるが、機密をたもったまま配送するためにはさらに他の機密管理機構が必要となる。また、全エンティティが共通の鍵を共有することは出来ない。更に、安全のため、自分の秘密アルゴリズムを変える場合、公開識別子を変える必要があり運用面での実用上、秘密アルゴリズムの再変更は困難である。

【０００４】したがって、本発明は想定される通信相手の数が多くても管理に多大な手間を要することがなく、不特定多数との暗号通信に適していて、全エンティティが共通の鍵を共有することが可能で、また、安全のため公開情報を変える場合、自分の秘密情報を変更する必要がなく、管理が容易で、かつ事前準備として各エンティティへ秘密アルゴリズムを配送する必要がなく、機密を保ったまま配送するために、さらに他の機密管理機構を必要とせず、安全のため、自分の秘密アルゴリズムを変える目的で、公開識別子を変えるなどの実用上困難な処理が必要ない共有暗号鍵による通信システム、同システム用サーバ装置、同システム用クライアント装置、及び通信システムにおける暗号鍵の共有方法を提供することを目的とする。

【０００５】

【課題を解決するための手段】本発明は上記目的を達成するために、従来のセンター管理暗号鍵共有方法では、共有する暗号鍵を変えるためにはクライアント側の暗証番号を変える必要があったのに対して、クライアント側の暗証番号は一定のまま、サーバの制御変数の変更のみで共有する暗号鍵を変更できるようにしている。このため、短い時間間隔で、共有する暗号鍵を変化させるシステム運用が可能となり、暗号システムの安全性が飛躍的に向上する。また、従来のセンター管理暗号鍵共有方法では、同じグループに属するすべてのクライアントで同じ暗号鍵を共有することはできなかったの対して、サーバの制御変数をある特定の値に設定することでサーバ所属のクライアントグループ内で同じ暗号鍵を共有できるようにしている。このため、緊急時など、特別な状況においてサーバの制御のみでグループ内の暗号化を解除することができる。

【０００６】すなわち本発明によれば、少なくともクライアントＡ、クライアントＢ、サーバＳ１により構成される共有暗号鍵による通信システムであって、前記クライアントＡは、予め定めた自分の暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］、並びに暗号鍵生成アルゴリズム［Ｋ］を保持する記憶手段と、前記暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ａ）を生成する手段と、生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知する手段と、前記クライアントＢとの共通鍵を生成するために、前記サーバＳ１へ前記クライアントＢの公開ｉｄを要求する手段と、前記サーバＳ１から送信される前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）と前記暗証番号ａを入力として前記暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｉ（ｂ），ｖ１），ａ）を生成する手段とを有し、前記クライアントＢは、予め定めた自分の暗証番号ｂ及び固有ｉｄ生成アルゴリズム［Ｉ］、並びに暗号鍵生成アルゴリズム［Ｋ］を保持する記憶手段と、前記暗証番号ｂ及び固有ｉｄ生成アルゴリズム［Ｉ］を用い

て固有ｉｄ　Ｉ（ｂ）を生成する手段と、生成された固有ｉｄ　Ｉ（ｂ）を前記サーバＳ１へ通知する手段と、前記サーバＳ１又は前記クライアントＡ及びクライアントＢが接続されたネットワーク経由で前記クライアントＡの公開ｉｄを入手し、前記クライアントＡの公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）と前記暗証番号ｂを入力として前記暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｉ（ａ），ｖ１），ｂ）を生成する手段とを有し、前記サーバＳ１は制御変数ｖ１を生成する手段と、前記クライアントＡから通知された固有ｉｄ　Ｉ（ａ）及び前記クライアントＢから通知された固有ｉｄＩ（ｂ）を保持するとともに、秘密で管理する前記制御変数ｖ１並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記クライアントＡからの要求を受けたときは、前記クライアントＢの固有ｉｄ　Ｉ（ｂ）と前記制御変数ｖ１と、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）を生成する手段と、生成された前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）を前記クライアントＡに送信する手段と、前記クライアントＡの固有ｉｄ　Ｉ（ａ）と前記制御変数ｖ１、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＡの前記公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）を生成する手段と、生成された前記公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）を前記クライアントＡに送信する手段とを有し、前記アルゴリズム［Ｉ］、［Ｓ］、［Ｋ］がＫ（Ｓ（Ｉ（ｂ），ｖ１），ａ）＝Ｋ（Ｓ（Ｉ（ａ），ｖ１），ｂ）を満足するものである共有暗号鍵による通信システムが提供される。

【０００７】さらに本発明によれば、請求項１記載の共有暗号鍵による通信システム用サーバ装置であって、制御変数ｖ１を生成する手段と、前記クライアントＡから通知された固有ｉｄＩ（ａ）及び前記クライアントＢから通知された固有ｉｄ　Ｉ（ｂ）を保持するとともに、秘密で管理する前記制御変数ｖ１並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記クライアントＡからの要求を受けたときは、前記クライアントＢの固有ｉｄ　Ｉ（ｂ）と前記制御変数ｖ１と、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）を生成する手段と、生成された前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）を前記クライアントＡに送信する手段と、前記クライアントＡの固有ｉｄ　Ｉ（ａ）と前記制御変数ｖ１、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＡの前記公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）を生成する手段と、生成された前記公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）を前記クライアントＡに送信する手段とを有する共有暗号鍵による通信システム用サーバ装置が提供される。

【０００８】さらに本発明によれば、請求項１記載の共有暗号鍵による通信システム用クライアント装置であって、予め定めた自分の暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］、並びに暗号鍵生成アルゴリズム［Ｋ］を保持する記憶手段と、前記暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ａ）を生成する手段と、生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知する手段と、前記クライアントＢとの共通鍵を生成するために、前記サーバＳ１へ前記クライアントＢの公開ｉｄを要求する手段と、前記サーバＳ１から送信される前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）と前記暗証番号ａを入力として前記暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｉ（ｂ），ｖ１），ａ）を生成する手段とを有する共有暗号鍵による通信システム用クライアント装置が提供される。

【０００９】さらに本発明によれば、少なくともクライアントＡ、クライアントＢ、サーバＳ１により構成される通信システムにおける暗号鍵の共有方法であって、前記クライアントＡが、前もって自分の暗証番号ａを定め、固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ａ）を生成するステップと、生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知するステップと、前記クライアントＢが、前もって自分の暗証番号ｂを定め、固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ｂ）を生成するステップと、生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知するステップと、前記クライアントＡが、前記クライアントＢとの共通鍵を生成するために、前記サーバＳ１へ前記クライアントＢの公開ｉｄを要求するステップと、前記サーバＳ１が前記クライアントＡからの要求を受け、保有している前記クライアントＢの固有ｉｄ　Ｉ（ｂ）と前記サーバが秘密で管理している制御変数ｖ１を入力として、公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）を生成するステップと、生成された前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）を前記クライアントＡに送信するステップと、前記サーバＳ１が、保有している前記クライアントＡの固有ｉｄ　Ｉ（ａ）とｖ１から前記クライアントＡの公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）を生成するステップと、生成された前記クライアントＡの公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）を前記クライアントＡに送信するステップと、前記クライアントＡが入手した前記クライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）と前記暗証番号ａを入力として暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｉ（ｂ），ｖ１），ａ）を生成するステップと、前記クライアントＢが前記サーバＳ１又は前記クライアントＡ及び前記クライアントＢの接続されたネットワーク経由で前記クライアントＡの公開ｉｄを入手し、暗号鍵　Ｋ（Ｓ（Ｉ（ａ），ｖ１），ｂ）を生成するステップとを有し、前記アルゴリズム［Ｉ］、

［Ｓ］、［Ｋ］がＫ（Ｓ（Ｉ（ｂ），ｖ１），ａ）＝Ｋ（Ｓ（Ｉ（ａ），ｖ１），ｂ）を満足するものである共有暗号鍵による通信システムにおける暗号鍵の共有方法が提供される。

【００１０】さらに本発明によれば、少なくともサーバＳ１に管理されるクライアントＡ、サーバＳ２に管理されるクライアントＣ、前記サーバＳ１と前記サーバＳ２を管理する親サーバＳ３により構成される共有暗号鍵による通信システムであって、前記クライアントＡは、予め定めた自分の暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］、並びに暗号鍵生成アルゴリズム［Ｋ］を保持する記憶手段と、前記暗証番号ａ及び前記固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ａ）を生成する手段と、生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知する手段と、前記クライアントＣとの共通鍵を生成するために、前記サーバＳ１へ前記クライアントＣの公開ｉｄを要求する手段と、前記サーバＳ１から送信される前記クライアントＣの３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）と前記暗証番号ａを入力として前記暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１），ａ）を生成する手段とを有し、前記クライアントＣは、予め定めた自分の暗証番号ｃ及び固有ｉｄ生成アルゴリズム［Ｉ］、並びに暗号鍵生成アルゴリズム［Ｋ］を保持する記憶手段と、前記暗証番号ｃ及び固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ｃ）を生成する手段と、生成された固有ｉｄ　Ｉ（ｃ）を前記サーバＳ２へ通知する手段と、前記クライアントＡ及びクライアントＣが接続されたネットワーク経由で前記クライアントＡの３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ａ），ｖ１），ｖ３），ｖ２）を入手し、前記クライアントＡの前記３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ａ），ｖ１），ｖ３），ｖ２）と前記暗証番号ｃを入力として前記暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ａ），ｖ１），ｖ３），ｖ２），ｃ）を生成する手段とを有し、前記サーバＳ１は前記クライアントＡから通知された固有ｉｄ　Ｉ（ａ）を保持するとともに、秘密で管理する制御変数ｖ１並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記クライアントＡからの要求を受けたときは、要求相手が自グループに属するか否かを判断する手段と、自グループに属さない要求相手のときは前記親サーバＳ３に前記クライアントＡからの要求を転送する手段と、前記親サーバＳ３から受信した前記クライアントＣの２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）と、前記制御変数ｖ１と、前記公開ｉｄ生成アルゴリズム［Ｓ］から前記３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）を生成して前記クライアントＡに送信する手段とを有し、前記サーバＳ２は前記クライアントＣから通知された固有ｉｄ　Ｉ（ｃ）を保持するとともに、秘密で管理する制御変数ｖ２並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記親サーバＳ３からの要求を受けたときは、前記クライアントＣの固有ｉｄ　Ｉ（ｃ）と前記制御変数ｖ２と、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＣの１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ２）を生成する手段と、生成された前記クライアントＣの１次公開ｉｄＳ（Ｉ（ｃ），ｖ２）を前記親サーバＳ３に送信する手段とを有し、前記親サーバＳ３は前記サーバＳ２から送信された前記クライアントＣの１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ２）を保持するとともに、秘密で管理する制御変数ｖ３並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記サーバＳ１からの要求を前記サーバＳ２に転送する手段と、前記サーバＳ２から前記クライアントＣの１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ２）を受けたときは、前記制御変数ｖ３と、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＣの前記２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）を生成する手段と、生成された前記クライアントＣの２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）を前記サーバＳ１に送信する手段とを有し、前記アルゴリズム［Ｉ］、［Ｓ］、［Ｋ］がＫ（Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１），ａ）＝Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ａ），ｖ１），ｖ３），ｖ２），ｃ）を満足するものである共有暗号鍵による通信システムが提供される。

【００１１】さらに本発明によれば、請求項５記載の共有暗号鍵による通信システム用サーバＳ１であって、前記クライアントＡから通知された固有ｉｄ　Ｉ（ａ）を保持するとともに、秘密で管理する制御変数ｖ１並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記クライアントＡからの要求を受けたときは、要求相手が自グループに属するか否かを判断する手段と、自グループに属さない要求相手のときは前記親サーバＳ３に前記クライアントＡからの要求を転送する手段と、前記親サーバＳ３から受信した前記クライアントＣの２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）と、前記制御変数ｖ１と、前記公開ｉｄ生成アルゴリズム［Ｓ］から前記３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）を生成して前記クライアントＡに送信する手段とを有する共有暗号鍵による通信システム用サーバ装置が提供される。

【００１２】さらに本発明によれば、請求項５記載の共有暗号鍵による通信システム用親サーバＳ３であって、前記サーバＳ２から送信された前記クライアントＣの１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ２）を保持するとともに、秘密で管理する制御変数ｖ３並びに公開ｉｄ生成アルゴリズム［Ｓ］を保持する記憶手段と、前記サーバＳ１からの要求を前記サーバＳ２に転送する手段と、前記サーバＳ２から前記クライアントＣの１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ２）を受けたときは、前記制御変数ｖ３

と、前記公開ｉｄ生成アルゴリズム［Ｓ］を用いて前記クライアントＣの前記２次公開ｉｄＳ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）を生成する手段と、生成された前記クライアントＣの２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）を前記サーバＳ１に送信する手段とを有する共有暗号鍵による通信システム用サーバ装置が提供される。

【００１３】さらに本発明によれば、請求項５共有暗号鍵による通信システム用クライアント装置であって、予め定めた自分の暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］、並びに暗号鍵生成アルゴリズム［Ｋ］を保持する記憶手段と、前記暗証番号ａ及び固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ａ）を生成する手段と、生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知する手段と、前記クライアントＣとの共通鍵を生成するために、前記サーバＳ１へ前記クライアントＣの公開ｉｄを要求する手段と、前記サーバＳ１から送信される前記クライアントＣの３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）と前記暗証番号ａを入力として前記暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１），ａ）を生成する手段とを有する共有暗号鍵による通信システム用クライアント装置が提供される。

【００１４】さらに本発明によれば、少なくともサーバＳ１に管理されるクライアントＡ、サーバＳ２に管理されるクライアントＣ、前記サーバＳ１と前記サーバＳ２を管理する親サーバＳ３により構成される通信システムにおける暗号鍵の共有方法であって、前記クライアントＡが、前もって自分の暗証番号ａを定め、固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ａ）を生成するステップと、生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ１へ通知するステップと、前記クライアントＣが、前もって自分の暗証番号ｃを定め、固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ｃ）を生成するステップと、生成された固有ｉｄ　Ｉ（ａ）を前記サーバＳ２へ通知するステップと、前記クライアントＡが、前記クライアントＣとの共通鍵を生成するために、前記サーバＳ１へ前記クライアントＣの公開ｉｄを要求するステップと、要求された通信相手である前記クライアントＣが自グループに属するか否かを前記サーバＳ１が判断するステップと、前記クライアントＣが自グループに属さないときは、前記サーバＳ１が前記親サーバＳ３へ前記クライアントＣの公開ｉｄを要求するステップと、前記親サーバＳ３が、前記サーバＳ１から要求された前記クライアントＣを管理するサーバＳ２へクライアントＣの公開ｉｄを要求するステップと、前記サーバＳ２が、保有している前記クライアントＣの固有ｉｄ　Ｉ（ｃ）と自らの制御変数ｖ２を入力としてアルゴリズム［Ｓ］を用いて、前記クライアントＣの１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ２）を生成するステップと、前記サーバＳ２が、生成された前記１次公開ｉｄを前記親サーバＳ３へ送信するステップと、前記親サーバＳ３が、前記１次公開ｉｄ　Ｓ（Ｉ（ｃ），ｖ２）と自らの制御変数ｖ３を入力としてアルゴリズム［Ｓ］を用いて、２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）を生成するステップと、前記親サーバＳ３が生成された前記２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）を前記サーバＳ１へ送信するステップと、前記サーバＳ１が前記２次公開ｉｄ　Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）と前記制御変数ｖ１と前記アルゴリズム［Ｓ］を用いて、３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）を生成するステップと、前記サーバＳ１が、生成された前記３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）を前記クライアントＡへ送信するステップと、前記クライアントＡが前記３次公開ｉｄ　Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）と前記暗証番号ａとアルゴリズム［Ｋ］を用いて暗号鍵Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１），ａ）を生成するステップと、前記クライアントＣが前記暗証番号ｃとアルゴリズム［Ｋ］を用いて暗号鍵Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ａ），ｖ１），ｖ３），ｖ２），ｃ）を生成するステップとを有し、前記アルゴリズム［Ｉ］、［Ｓ］、［Ｋ］がＫ（Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１），ａ）＝Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ａ），ｖ１），ｖ３），ｖ２），ｃ）を満足するものである共有暗号鍵による通信システムにおける暗号鍵の共有方法が提供される。

【００１５】

【発明の実施の形態】以下、本発明の共有暗号鍵による通信システム、同システム用サーバ装置、同システム用クライアント装置、及び通信システムにおける暗号鍵の共有方法の実施の形態を好ましい実施例によって図面に従い詳細に説明する。図１は、本発明の共有暗号鍵による通信システムの一例を示すブロック図である。本発明の適用される暗号通信のネットワークは、２つ以上のクライアントと１つ以上のサーバから構成されており、クライアントはいずれかのサーバに所属している。また、図１の例のようにサーバが複数ある場合、これらは論理的な階層構造でネットワーク化されており、下位のサーバはいずれかの上位サーバに所属する。下位サーバを収容する上位サーバを親サーバと呼び、同じ親サーバに所属する下位サーバとクライアント群をグループと呼ぶ。なお、クライアントにおけるソフトウェアを含んだハードウェアをクライアント装置といい、同様にサーバにおけるソフトウェアを含んだハードウェアをサーバ装置という。なお、本発明はサーバの数によって制限を受けるものではないが、一般的にはネットワークに分散配置された、公開ｉｄを管理する複数のサーバを有するシステムに適用可能である。

【００１６】サーバより共有暗号鍵を生成するためのサービスを受け、共有暗号鍵を生成した後、それを用いて暗号化通信を行う主体であるクライアントには、コンピュータ、ＩＣカード、移動体通信機等、全ての通信・情報処理装置が該当する。また、クライアントに対し共有暗号鍵を生成するためのサービスを提供する主体であるサーバにはコンピュータ、移動体通信制御装置等、全ての通信・情報処理装置が該当する。なお、各クライアント、サーバはＣＰＵ（中央演算処理装置）、メモリ、インターフェース他を有し、所定の通信機能、データ保持機能を有しているものとする。なお、ネットワークを構成する通信回線は、公衆回線、高速デジタル回線などの有線のみならず、電波や光などを用いた無線通信も含まれ、有線と無線の組合わせも含まれる。

【００１７】全てのクライアントは公開可能な暗号鍵生成アルゴリズム［Ｋ］と固有ｉｄ生成アルゴリズム［Ｉ］を共通に持つ。固有ｉｄとは、各クライアントが秘密で保有する暗証番号を入力としてアルゴリズム［Ｉ］により生成される値で、クライアントにより生成され、サーバへ送信の後、サーバで管理される。なお、暗証番号は、必ずしも数字のみならず、文字を含むことができる。また、アルゴリズム［Ｉ］の非可逆性により、固有ｉｄから暗証番号への逆変換は困難である。全てのサーバは公開可能な公開ｉｄ生成アルゴリズム［Ｓ］を共通に持つ。公開ｉｄとは、クライアントの固有ｉｄとサーバの制御変数を入力としてアルゴリズム［Ｓ］により生成される値で公開可能な値である。図２は、図１中のサーバＳ１と、これによって管理される複数のクライアント中の２つであるクライアントＡとクライアントＢがそれぞれ有する各アルゴリズムを模式的に示す図である。

【００１８】次に暗号鍵の生成の手順について図２の例、すなわち同一のサーバＳ１に所属するクライアントＡ及びクライアントＢが鍵を生成する場合を第１実施例として説明する。図３は第１実施例の模式図である。また、図４は図３の実施例におけるクライアントＡのＣＰＵの動作を説明するフローチャートであり、図５は図３の実施例におけるサーバＳ１のＣＰＵの動作を説明するフローチャートである。

【００１９】

【表３】

（１）　クライアントＡは、前もって自分の暗証番号ａを定め、固有ｉｄ生成アルゴリズム［Ｉ］を用いて固有ｉｄ　Ｉ（ａ）を生成し、サーバＳ１へ通知しておく。クライアントＢも同様に固有ｉｄ　Ｉ（ｂ）をサーバへ通知しておく。

（２）　クライアントＡは、クライアントＢとの共通鍵を生成するために、サーバＳ１へクライアントＢの公開ｉｄを要求する。

（３）　サーバＳ１はクライアントＡからの要求を受け、保有しているクライアントＢの固有ｉｄ　Ｉ（ｂ）とサーバが秘密で管理している制御変数ｖ１を入力として、公開ｉｄ生成アルゴリズム［Ｓ］を用いてクライアントＢの公開ｉｄＳ（Ｉ（ｂ），ｖ１）を生成しクライアントＡに通知する。

（４）　同時に、サーバＳ１は、保有しているクライアントＡの固有ｉｄ　Ｉ（ａ）とｖ１からクライアントＡの公開ｉｄ　Ｓ（Ｉ（ａ），ｖ１）を生成しクライアントＡに通知する。

（５）　クライアントＡは入手したクライアントＢの公開ｉｄ　Ｓ（Ｉ（ｂ），ｖ１）と自分の秘密の暗証番号ａを入力として暗号鍵生成アルゴリズム［Ｋ］を用いて暗号鍵　Ｋ（Ｓ（Ｉ（ｂ），ｖ１），ａ）を生成する。

（６）　クライアントＢはサーバＳ１経由で又は、クライアントＡ及びクライアントＢが接続されたネットワーク経由でクライアントＡの公開ｉｄを入手し、暗号鍵Ｋ（Ｓ（Ｉ（ａ），ｖ１），ｂ）を生成する。

【００２０】次に上記方法で生成された暗号鍵を両クライアントＡ、Ｂで共有する手法について説明する。クライアントＡとクライアントＢで暗号鍵を共有するためには、Ｋ（Ｓ（Ｉ（ｂ），ｖ１），ａ）＝Ｋ（Ｓ（Ｉ（ａ），ｖ１），ｂ）・・・式①が成立する様なアルゴリズム［Ｉ］、［Ｓ］、［Ｋ］を用いればよい。

【００２１】

【数１】この点について具体例を挙げて説明すると、例えば、ｐを素数、ｇをｍｏｄｐにおける原始根として

［Ｉ］：Ｉ（ｘ）＝g^{X} ｍｏｄ　ｐ

［Ｓ］：Ｓ（ｘ１，ｘ２）＝$x1^{X2}$ ｍｏｄ　ｐ

［Ｋ］：Ｋ（ｘ１，ｘ２）＝$x1^{X2}$ ｍｏｄ　ｐ

とすると

Ｋ（Ｓ（Ｉ（ｂ），ｖ１），ａ）

＝Ｋ（Ｓ（g^{b} ｍｏｄ　ｐ，ｖ１），ａ）

＝Ｋ（（g^{b} ｍｏｄ　ｐ）^{V1} ｍｏｄ　ｐ，ａ）

＝Ｋ（（$g^{b\cdot v1}$ ｍｏｄ　ｐ），ａ）

＝（$g^{b\cdot v1}$ ｍｏｄ　ｐ）^{a} ｍｏｄ　ｐ

＝$g^{b\cdot v1\cdot a}$ ｍｏｄ　ｐ

【００２２】

【数２】同様に

Ｋ（Ｓ（Ｉ（ａ），ｖ１），ｂ）＝$g^{a\cdot v1\cdot b}$ ｍｏｄ　ｐ

となる。$g^{b\cdot v1\cdot a} \equiv g^{a\cdot v1\cdot b}$ （ｍｏｄ　ｐ）　であるから式①は成立し、クライアントＡとクライアントＢは暗号鍵を共有できる。

【００２３】次に上記の手法で生成された暗号鍵により暗号化されたデータあるいは通信文を解読して平文化するために必要な暗号鍵の解除方法について説明する。ここではサーバＳ１に所属するクライアントＡ及びクライアントＢが生成する共通鍵をサーバＳ１からの制御により特定の値とする方法について説明する。共通鍵を特定の値とすることは実質的に暗号化の解除を意味し、クライアント側の特別な手続き無しでサーバ側の制御のみで

可能であることが本方法の特徴である。先に説明した通り、クライアントＡは共通鍵としてＫ（Ｓ（Ｉ（ｂ），ｖ１），ａ）を生成するが、ａ及びｂは各々のクライアントのみが知る値でサーバが自由に制御できるのは制御変数ｖ１のみである。

【００２４】

【数３】したがって、ａ及びｂの値のいかんに関わらずｖ１に対して特定の値を生み出すアルゴリズム［Ｋ］及び［Ｓ］を採用することで共通鍵を特定の値とすること

$$g^{b\cdot v1\cdot a} \equiv g^{b\cdot \hat{}\,\psi(p)\cdot a} \equiv (g^{b\cdot a})\hat{}\,\psi(p) \equiv 1 \pmod{p}$$

となり、特定の値　１を持つ（記号”＾ψ(ｐ)”は”ψ(ｐ)乗”を示す：以下同じ）。同様に、クライア

$$K(S(I(a),v1),b) = g^{a\cdot v1\cdot b} \equiv 1 \pmod{p}$$

となり、共通鍵を特定の値　１に制御できる。

【００２５】上記第１実施例の動作をクライアントＡのクライアント装置に用いられるＣＰＵの動作を示す図４のフローチャートとサーバＳ１のサーバ装置に用いられるＣＰＵの動作を示す図５のフローチャートに沿って説明する。図４において、図示省略の所定のイニシャライズの後、ステップＳ１０で通信要求の有無を検出し、要求があれば、ステップＳ１１でサーバＳ１に接続する。いまクライアントＡからクライアントＢへの通信を行うものとし、ステップＳ１２でサーバＳ１に対して通信相手であるクライアントＢと自分（クライアントＡ）の公開ｉｄを要求する。ここでサーバＳ１は図５のステップＳ３０、Ｓ３１を経てクライアントＡからの要求を読み込み、クライアントＢとクライアントＡの公開ｉｄをそれぞれ生成し（ステップＳ３２、Ｓ３３）、ステップＳ３４でクライアントＡに送信する。ステップＳ３５は正常に送信が終了したか否かを判断するもので、正常でなければ、ステップＳ３１から再度実行する。

【００２６】図４のステップＳ１３では、サーバＳ１から上記２つの公開ｉｄを受信したか否かを判断し、受信したときはサーバＳ１との通信を終了し（ステップＳ１４）、次いで自分の暗証番号ａを読み出して（ステップＳ１５）、通信相手の公開ｉｄとアルゴリズム［Ｋ］を用いて暗号鍵を生成する（ステップＳ１６）。次にクライアントＢへ送信すべき通信文、すなわち電文を暗号鍵と所定の暗号化アルゴリズムに従って暗号化する（ステップＳ１７）。暗号化が終了すると、通信相手又はネットワークに接続し、暗号文を送信する（ステップＳ１８、Ｓ１９、Ｓ２０）。送信が正常に終了しないときはステップＳ２１経由でステップＳ１９、Ｓ２０を再度実行する。なお、ネットワークに接続した場合は直接クライアントＢに送信するのではなく、所定サーバのメモリに暗号文が保持され、クライアントＢが、その後そのサーバにアクセスしてこれを取り出すこととなる。

【００２７】次に異なるグループ間の鍵の共有方法について第２実施例として説明する。この第２実施例はサーバＳ１に属するクライアントＡとサーバＳ２に属するクライアントＣの鍵共有を説明する。なお、図６に示すようにサーバＳ１及びＳ２の親サーバをＳ３とする。また、クライアントＡの固有ｉｄ　Ｉ（ａ）はサーバＳ１に、クライアントＣの固有ｉｄ　Ｉ（ｃ）はサーバＳ２に事前に通知されているものとする。

【００２８】

【表４】第２実施例における動作は次のようになる。

（１）　クライアントＡはサーバＳ１にクライアントＣの公開ｉｄを要求する。

（２）　サーバＳ１はクライアントＣが自グループでないので親サーバＳ３へクライアントＣの公開ｉｄを要求する。

（３）　親サーバＳ３は、クライアントＣを管理するサーバＳ２へクライアントＣの公開ｉｄを要求する。なお、クライアントＣを管理するサーバがＳ２であることはクライアント名の名付けに例えば、Ｃ－Ｓ２－Ｓ３の様な論理的な階層構造を表す方法を採用することで容易に実現できる。

（４）　サーバＳ２は、保有しているクライアントＣの固有ｉｄ　Ｉ（ｃ）と自らの制御変数ｖ２を入力としてアルゴリズム［Ｓ］を用いて、Ｓ（Ｉ（ｃ），ｖ２）を生成し、親サーバＳ３へ通知する。

（５）　親サーバＳ３は、Ｓ（Ｉ（ｃ），ｖ２）と自らの制御変数ｖ３を入力としてアルゴリズム［Ｓ］を用いて、Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３）を生成し、サーバＳ１へ通知する。

（６）　サーバＳ１も同様に、Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１）を生成し、クライアントＡへ通知する。

（７）　クライアントＡはアルゴリズム［Ｋ］を用いて暗号鍵Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ｃ），ｖ２），ｖ３），ｖ１），ａ）を生成する。

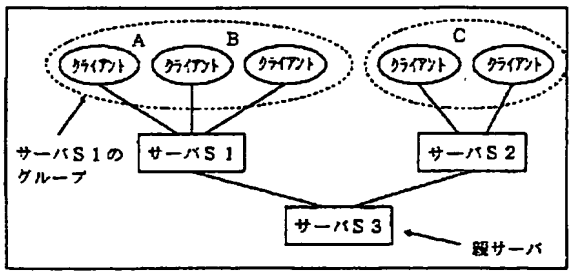
（８）　クライアントＣも同様に、暗号鍵Ｋ（Ｓ（Ｓ（Ｓ（Ｉ（ａ），ｖ１），ｖ３），ｖ２），ｃ）を生成する。

【００２９】
【数４】前述のアルゴリズム
［Ｉ］：Ｉ（ｘ）＝g^X ｍｏｄ ｐ
［Ｓ］：Ｓ（ｘ１，ｘ２）＝$x1^{X2}$ ｍｏｄ ｐ
［Ｋ］：Ｋ（ｘ１，ｘ２）＝$x1^{X2}$ ｍｏｄ ｐ
の場合、

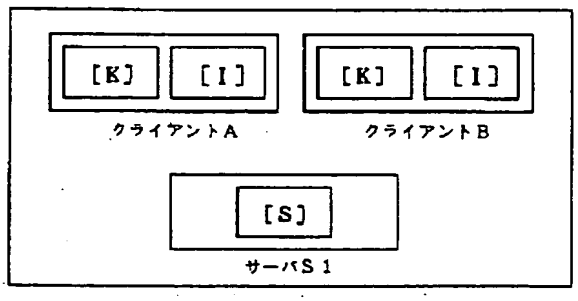
$$K(S(S(S(I(c),v2),v3),v1),a)$$
$$=K(S(S(S(g^c \bmod p),v2),v3),v1),a)$$
$$=K(S(S(g^{c\cdot v2} \bmod p),v3),v1),a)$$
$$=K(S(g^{c\cdot v2\cdot v3} \bmod p),v1),a)$$
$$=K(g^{c\cdot v2\cdot v3\cdot v1} \bmod p),a)$$
$$=g^{c\cdot v2\cdot v3\cdot v1\cdot a} \bmod p$$

また、同様に
$K(S(S(S(I(a),v1),v3),v2),c)=g^{a\cdot v1\cdot v3\cdot v2\cdot c} \bmod p$
$g^{c\cdot v2\cdot v3\cdot v1\cdot a} \equiv g^{a\cdot v1\cdot v3\cdot v2\cdot c}$ （ｍｏｄ ｐ）であるからグループの異なるクライアント間でも暗号鍵を共有できることがわかる。
【００３０】上記各実施例では、２つのクライアント間の通信について説明したが、クライアント数が増加しても、同様の原理で暗号の共有化を図ることができる。また、ネットワークが図１に示した構成よりさらに複雑化して、サーバが３段以上の階層に配された場合でも同様に暗号の共有化を図ることができる。
【００３１】
【発明の効果】本発明の共有暗号鍵による通信システム、同システム用サーバ装置、同システム用クライアント装置、及び通信システムにおける暗号鍵の共有方法は上記のように構成されているので、次のような効果を有する。すなわち、従来のセンター管理暗号鍵共有方法では、共有する暗号鍵を変えるためにはクライアント側の暗証番号を変える必要があったが、本方法ではクライアント側の暗証番号は一定のまま、サーバの制御変数の変更のみで共有する暗号鍵を変更できる。このため、短い時間間隔で、共有する暗号鍵を変化させるシステム運用が可能となり、暗号システムの安全性が飛躍的に向上する。また、従来のセンター管理暗号鍵共有方法では、同じグループに属するすべてのクライアントで同じ暗号鍵を共有することはできなかったが、本方法ではサーバの制御変数をある特定の値に設定することでサーバ所属のクライアントグループ内で同じ暗号鍵を共有できる。このため、緊急時など、特別な状況においてサーバの制御のみでグループ内の暗号化を解除することができる。
【図面の簡単な説明】
【図１】本発明の共有暗号鍵による通信システムの適用される通信ネットワーク例を模式的に示すブロック図である。
【図２】図１中のサーバＳ１と、これによって管理される複数のクライアント中の２つであるクライアントＡとクライアントＢがそれぞれ有する各アルゴリズムを模式的に示す図であり、本実施例の第１実施例に対応する図である。
【図３】本発明の第１実施例における動作を模式的に示す図である。
【図４】本発明の第１実施例におけるクライアントのＣＰＵの動作を模式的に示すフローチャートである。
【図５】本発明の第１実施例におけるサーバのＣＰＵの動作を模式的に示すフローチャートである。
【図６】本発明の第２実施例における動作を模式的に示す図である。
【図７】従来の暗号鍵共有方法の１つを示す模式図である。
【図８】従来の暗号鍵共有方法の１つを示す模式図である。
【図９】従来の暗号鍵共有方法の１つを示す模式図である。
【符号の説明】
Ａ、Ｂ、Ｃ　クライアント装置
Ｓ１、Ｓ２、Ｓ３　サーバ装置

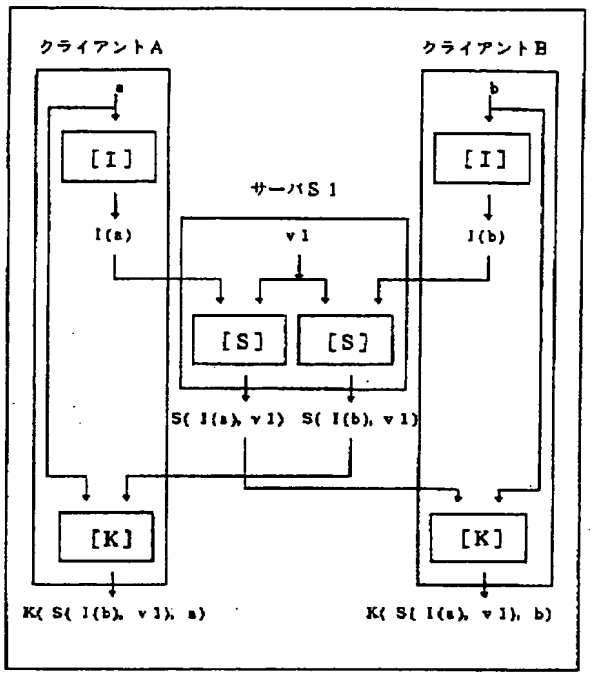
【図１】



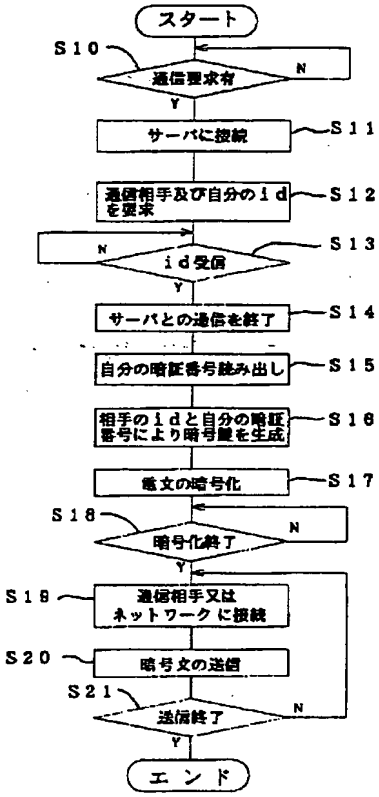
【図２】



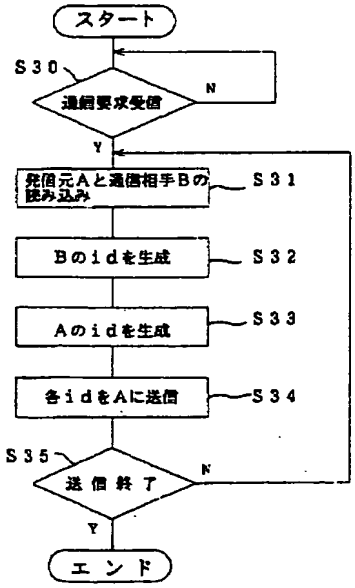
【図３】


クライアントA
クライアントB
a
b
[I]
[I]
サーバS１
I(a)
v1
I(b)
[S]
[S]
S(I(a), v1)
S(I(b), v1)
[K]
[K]
K(S(I(b), v1), a)
K(S(I(a), v1), b)

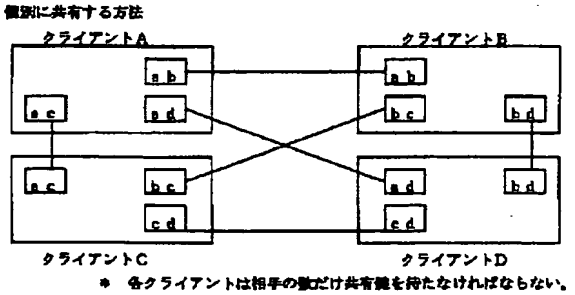
【図４】


スタート
S10
通信要求有
N
Y
サーバに接続
S11
通信相手及び自分のｉｄを要求
S12
N
ｉｄ受信
S13
Y
サーバとの通信を終了
S14
自分の暗証番号読み出し
S15
相手のｉｄと自分の暗証番号により暗号鍵を生成
S16
原文の暗号化
S17
S18
暗号化終了
N
Y
S19
通信相手又はネットワークに接続
S20
暗号文の送信
S21
送信終了
N
Y
エンド

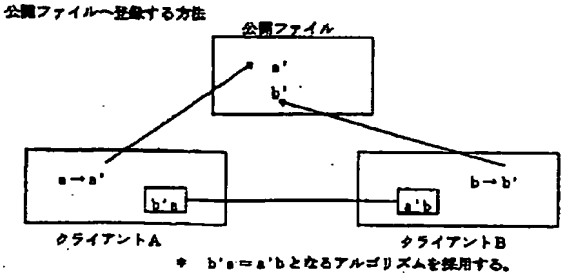
【図５】


スタート
S30
通信要求受信
N
Y
発信元Aと通信相手Bの読み込み
S31
Bのｉｄを生成
S32
Aのｉｄを生成
S33
各ｉｄをAに送信
S34
S35
送信終了
N
Y
エンド

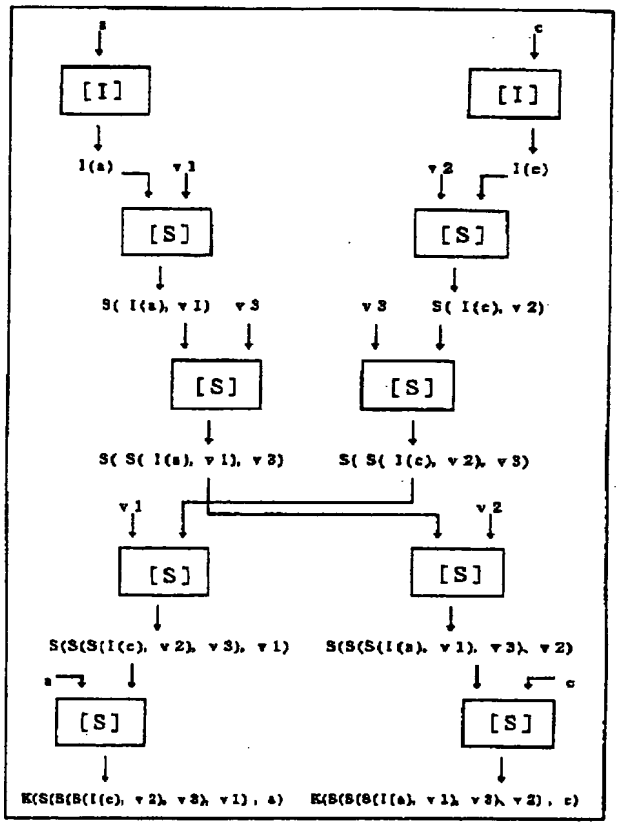
【図７】


個別に共有する方法
クライアントA
クライアントB
a b
a c
a d
b c
b d
a c
b c
c d
a d
b d
c d
クライアントC
クライアントD
＊　各クライアントは相手の数だけ共有鍵を持たなければならない。

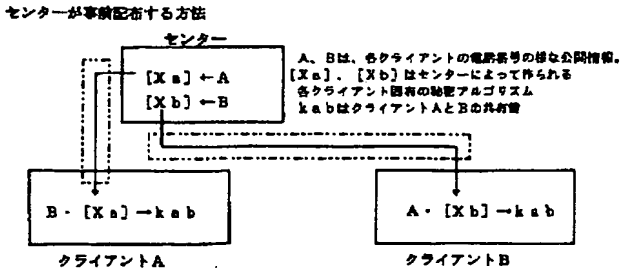
【図８】


公開ファイルへ登録する方法
公開ファイル
a'
b'
a→a'
b→b'
b'a
a'b
クライアントA
クライアントB
＊　b'a＝a'bとなるアルゴリズムを採用する。

【図６】


a
c
[I]
[I]
I(a)
v1
v2
I(c)
[S]
[S]
S(I(a), v1)　v3
v3　S(I(c), v2)
[S]
[S]
S(S(I(a), v1), v3)
S(S(I(c), v2), v3)
v1
v2
[S]
[S]
S(S(S(I(c), v2), v3), v1)
S(S(S(I(a), v1), v3), v2)
a
c
[S]
[S]
E(S(S(S(I(c), v2), v3), v1), a)
E(S(S(S(I(a), v1), v3), v2), c)

【図９】


センターが事前配布する方法
センター
[Xa] ←A
[Xb] ←B
A、Bは、各クライアントの電話番号の様な公開情報。
[Xa]、[Xb]はセンターによって作られる
各クライアント固有の秘密アルゴリズム
kabはクライアントAとBの共有鍵
B・[Xa] →kab
A・[Xb] →kab
クライアントA
クライアントB